

[Company]

LOGGING AND MONITORING POLICY

System monitoring and logging

Last Reviewed: [Last Reviewed] Page 1 of 12



1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

Last Reviewed: [Last Reviewed] Page 2 of 12



2 Document Contents Page

1	Doo	ocument Version Control		
2	Doo	ocument Contents Page		
3	Log	ging and Monitoring Policy	. 5	
	3.1	Purpose	.5	
	3.2	Scope	. 5	
	3.3	Principle	. 5	
	3.4	Event Logging	. 6	
	3.5	Event Logging Access Control	.7	
	3.6	Protection of Event Log Information	.7	
	3.7	Administrator and operator logs	.8	
	3.8	Clock synchronisation	. 8	
	3.9	Event Log Monitoring	. 8	
	3.10	Event Log Retention	. 9	
	3.11	Centralised Logging	.9	

Last Reviewed: [Last Reviewed]

LOGGING AND MONITORING POLICY



Version: [Version Number] Classification: Internal

	3.12	Personal Privacy	9
4	Pol	icy Compliance	. 10
	4.1	Compliance Measurement	. 10
	4.2	Exceptions	. 10
	4.3	Non-Compliance	. 10
	4.4	Continual Improvement	. 10
5	Are	eas of the ISO27001 Standard Addressed	. 11

📊 HighTable

Version: [Version Number] Classification: Internal

3 Logging and Monitoring Policy

3.1 Purpose

The purpose of this policy is to address the identification and management of risk the

of system-based security events by logging and monitoring systems.

To record events and gather evidence.

3.2 Scope

All company employees and external party users.

All devices used to process, store, or transmit company information.

3.3 Principle

All devices that process, store, or transmit confidential, card holder or personal

information have audit and logging enabled, where logging is possible and practical

and can generate audit logs.

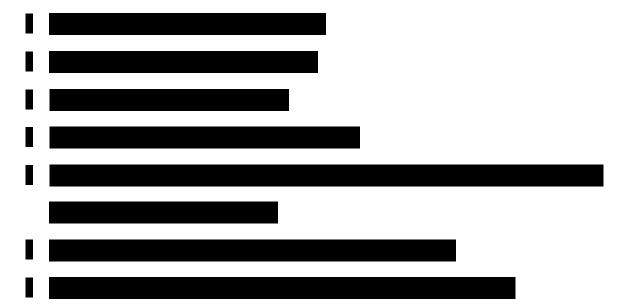


3.4 Event Logging

Event logs recording user activities, exceptions, faults, and information security events should be produced, kept, and regularly reviewed.

Event logs should include, when relevant:

- user IDs.
- system activities.
- dates, times, and details of key events, e.g., log-on and log-off.
- device identity or location if possible and system identifier.
- records of successful and rejected system access attempts.
- records of successful and rejected data and other resource access attempts.
- changes to system configuration.
- use of privileges.



Last Reviewed: [Last Reviewed] Page 6 of 12



Automated monitoring systems which can generate consolidated reports and alerts on system security are used where possible.

3.5 Event Logging Access Control

Event logging and monitoring is performed by authorised personnel only.

Event logging and monitoring systems and reports are

Where possible, system administrators should not have permission to

3.6 Protection of Event Log Information

Logging facilities and log information should be protected against tampering and unauthorized access.

Controls protect against unauthorized changes to log information and operational problems with the logging facility including:

- alterations to the message types that are recorded
- log files being edited or deleted

•

Last Reviewed: [Last Reviewed] Page 7 of 12



3.7 Administrator and operator logs

System administrator and system operator activities should be
Privileged user account holders may be
An intrusion detection system managed outside of the control of system and network
administrators can be used to

3.8 Clock synchronisation

The clocks of all relevant information processing systems within an organization or security domain should be synchronised to a single reference time source.

3.9 Event Log Monitoring

Responsibilities are assigned for the analysing and monitoring of events.

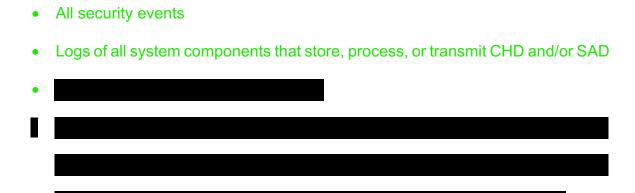
High risk events automatically alert to the incident management process.

Log files are

Last Reviewed: [Last Reviewed] Page 8 of 12



The following shall be reviewed daily:



3.10 Event Log Retention

Event logs from the immediately available.

Event logs are retained for

3.11 Centralised Logging

Centralised logging to a remote dedicated log server should be considered.

3.12 Personal Privacy

Privacy of employees and customers is respected in line with legal and regulatory requirement, including but not limited to

Last Reviewed: [Last Reviewed] Page 9 of 12

📊 HighTable

Version: [Version Number] Classification: Internal

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy

through various methods, including but not limited to, business tool reports, internal

and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information

Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action,

up to and including termination of employment.

4.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.

Last Reviewed: [Last Reviewed]

Page 10 of 12